Information Security Core Technology Status

	Business Driver	Security Solution	Vendor/Product Brand	Purchased/Source	Remaining Costs	SFA Rollout	Recommendations
1	Internet and Extranet Network Perimeter Protection	Network/Firewall Access	Cisco Router ACLs, Nokia/Checkpoint Firewall-1	Enterprise License	Demand Dependent	100%	Maintain current product line
2	Quickly identify intrusions to our network resources from the Internet	Intrusion Detection - External/Internet	Tripwire	Enterprise License	TBD-Contract Product and Services	Rollout 50% Complete	ISS RealSecure & ISS SAFEsuite Decisions – www.iss.net
3	Quickly identify intrusions to our network resources from internal employees & contractors	Intrusion Detection - Internal	Tripwire	Enterprise License	TBD-Contract Product and Services	Rollout 50% Complete	ISS RealSecure & ISS SAFEsuite Decisions – www.iss.net
4	Ensure SFA has capability to respond to intrusions and minimize damage/enhance disaster recovery	Computer Emergency Response Team (CERT)	Global Mgmt Center Detection, no response capability		Demand Dependent	None	Augment Data Center with CERT Team or WAR Room
5	Ensure host servers maintain security compliance and build standards	Server Compliance and detection	None	None	TBD-Contract Product and Services	None	ISS System Scanner – www.iss.net, Axent Enterprise Security Manager – www.axent.com
6	Ensure network devices maintain security compliance and standards	Network Compliance and Detection	None	None	TBD-Contract Product and Services	None	ISS System Scanner – www.iss.net, Axent Enterprise Security Manager – www.axent.com
7	Actively penetrate systems to assess hacker exploits	Penetration Study	KPMG/CSC	Routine	Demand Dependent	Currently being done by the IG, validating findings. KPMG/CSC establishing routine tests	Tool Suggestions: Nmap – www.insecure.org/nmap, Nessus – www.nessus.org - Linux ISS Internet Scanner – www.iss.net
8	Collect data on logon events for fraud and audit needs	Central Reporting & Logging of Security Events	None	None	TBD-Contract Product and Services	None	IBM Policy Director or eSecurity

US DEPARTMENT OF EDUCATION
STUDENT FINANCIAL ASSISTANCE
SFA MODERNIZATION PARTNER

ITA DETAILED DESIGN DOCUMENT
VOLUME 5
SECURITY ARCHITECTURE

Information Security Core Technology Status

	Business Driver	Security Solution	Vendor/Product Brand	Purchased/Source	Remaining Costs	SFA Rollout	Recommendations
9	Provide central authentication and authorization services for Internet users (20million +)	Internet Customer Authentication	Various spot solutions, no central function, BMC Control SA	BMC, TBD Depending on requirements	TBD-Contract Product and Services	None	IBM Policy Director, Encommerce Get Access
10	Provide central policy enforcement and decisioning	Central Policy Direction and Control	None	None	TBD	None	IBM Policy Director, Encommerce Get Access
11	Mechanism for ensuring key decision implementers are controlled, audited, and follow SFA processes	Operating System and Privileged User Controls	None	None	None	None	Axent UPM Product, www.axent.com
12	Security of telecommunications systems	PBX/VRU/ACD Security	None	None	TBD-Contract Product and Services	None	SecureLogix - Telewall/Telesweep, www.securelogix.com
13	Provide communications level security	Middleware Security (MQ, CORBA, etc)	None	None	None	None	IBM Policy Director or Candle Corporation
14	Remote System Access for production support, email,	Secure Dialup and VPN	Cisco 5300s, Cisco Secure RADIUS, Chatterbox/PCAnywhere (migrating Citrix)	Enterprise License	Demand Dependent	100%	Maintain current product line
15	Provide central employee directory for single signon and automated password reset	Directory Services (LDAP)	Netscape - Test	Two Server	TBD-Pending production definition	Test/Prototype	IBM LDAP {free}, Netscape, ICL
16	Secure key SFA databases and customer information	Database Security	Native Oracle Security functions, no security implemented on other RDBMSs	Oracle	Unknown	One Server completed	Implement natively purchased dBase security, ISS Database Scanner – www.iss.net
17	Ensure SFA and customer proprietary information is securely emailed and/or free of prioprietary content	None	None	None	None	None	Provide requirement to Department of Education who controls email
18	Ensure SFA systems are not negated or infected with viruses	Virus Protection	MCAfee and CA Innoculan	Enterprise License	Demand Dependent	Currently Implemented	Maintain current product line